REMARKS

This Amendment is fully responsive to the final Office Action dated November 21, 2008, issued in connection with the above-identified application. Claims 1, 2, 4, 5 and 10-12 are pending in the present application. With this Amendment, claims 1, 2, 11, and 12 have been amended. However, the amendments made to the claims are meant for clarification and are not meant to narrow the scope of the claims. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is respectfully requested.

I. Claim Rejection under 35 U.S.C. § 103(a)

A. Claims 1, 2, 5, and 10-12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Diffie et al. (U.S. Patent No. 5,371,794, hereafter "Diffie") in view of Devadas et al. (U.S. 2003/0204743, hereafter "Devadas"). The Applicants traverse the rejection for at least the reasons noted below. The Applicants assert that the cited prior art fails to disclose or suggest at least the features recited in independent claims 1, 2, 11 and 12.

For example, claim 1 recites the features of an encrypted communication system comprising a first device and a second device. The first device (i) encrypts a first key using a public key of the second device to generate first encrypted data, and transmits the first encrypted data to the second device, (ii) receives second encrypted data from the second device, the second encrypted data being generated by encrypting a third key of the second device using a public key of the first device at the second device, and decrypts the second encrypted data using a secret key of the first device to obtain a second key, and (iii) generates, based on the first and second keys, a first encryption key for use in communication with the second device.

As recited in claim 1, the second device (i) encrypts the third key using the public key of the first device to generate the second encrypted data, and transmits the second encrypted data to the first device, (ii) receives the first encrypted data from the first device, and decrypts the first encrypted data using a secret key of the second device to obtain a fourth key, and (iii) generates, based on the third and fourth keys, a second encryption key for use in communication with the first device. The first and second devices perform encrypted communication using the first and second encryption keys. The first device generates the first encryption key and a first hash key

based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device. The first encryption key is distinct from the first hash key.

The second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value. The second encryption key is distinct from the second hash key.

The features noted above in independent claim 1 are similarly recited in independent claims 2, 11 and 12. Specifically, claim 2 recites a related communication device, claim 11 recites a related method, and claim 12 recites a related computer program.

In the Office Action, the Examiner relies on the combination of Diffie and Devadas for disclosing or suggesting all the features recited in independent claims 1, 2, 11 and 12. However, the Applicants assert that the cited prior art does not teach or suggest the above-noted combination of features recited in amended independent claims 1, 2, 11 and 12.

Diffie discloses a method and apparatus for providing a secure wireless communication link between a mobile nomadic device (a mobile) and a base computing unit (a base). The mobile sends to the base a host certificate (Cert Mobile). When the base determines that the Cert Mobile is valid, the base sends to the mobile a Cert Base, and random number (RN1) encrypted in mobile's pubic key. The base saves the RN1 value. When the mobile validates the Cert Base, the mobile determines the RN1 value by decrypting the encrypted RN1 using the mobile's private key. The mobile generates RN2 and generates the session key from RN1 and RN2, and encrypts RN2 using the base's public key. The mobile sends to the base the encrypted RN2, and the base decrypts the encrypted RN2 using the base's private key. The base determines the session key

from RN1 and RN2. The mobile and the base enter a data transfer phase using encrypted data that is decrypted using the session key which is RN1 and RN2 (see e.g., abstract and Figs. 5a and 5b).

However, Diffie fails to disclose a system in which the first device generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device.

Additionally, Diffie fails to disclose a second device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered with when the received first hash value matches the calculated second hash value, as recited in independent claim 1.

Similarly, Diffie fails to disclose a communication device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for transmission data, encrypts the transmission data using the first encryption key to generate encrypted transmission data, and transmits the first hash value and the encrypted transmission data to the other device, as recited in independent claim 2.

Diffie also fails to disclose a communication device that receives from the other device a second hash value for second transmission data and encrypted second transmission data, and the other device that generates the second encryption key and a second hash key based on the third and fourth keys, calculates using the second hash key the second hash value for the second transmission data, encrypts the second transmission data using the second encryption key to generate encrypted second transmission data, and transmits the second hash value and the encrypted second transmission data to the communication device, as recited in independent claims 2.

Diffie further fails to disclose a communication device that decrypts the encrypted second transmission data using the first encryption key, calculates using the first hash key a second hash value for the decrypted second transmission data, and determines that the second transmission data is not tampered when the received second hash value matches the calculated second hash value, as recited in independent claims 2.

In the Office Action, the Examiner admits that Diffie fails to disclose a first device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, as well as, a second device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value. Thus, independent claims 1, 2, 11 and 12 are clearly distinguished over the Diffie reference.

However, the Examiner relies on Devadas regarding that which the Examiner admits (noted above) is lacking in the Diffie. Regarding the Devadas, the Applicants note that paragraph [0212] of the reference teaches that owner 234 sends an old challenge and a new prechallenge to CPUF chip 48. The new prechallenge is passed through hash module 191 to generate a new challenge. The new challenge is passed through PUF circuit 100 to generate a new response. On the other hand, the old challenge is passed through PUF circuit 100 to generate an old response. The old response is passed through a hash module h2 193 to generate a secret key. The secret key is used by encryption and MAC module 195 to encrypt the message and generate a MAC for the encrypted message. The encrypted message and the MAC is sent out of the chip and forwarded to owner 234.

However, Devadas fails to disclose a system in which the first device generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device

Additionally, Devadas fails to disclose a second device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value, as recited in independent claim 1.

Similarly, Devadas fails to disclose a communication device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for transmission data, encrypts the transmission data using the first encryption key to generate encrypted transmission data, and transmits the first hash value and the encrypted transmission data to the other device, as recited in independent claim 2. Devadas also fails to disclose a communication device that receives from the other device a second hash value for second transmission data and encrypted second transmission data, the other device generates the second encryption key and a second hash key based on the third and fourth keys, calculates using the second hash key the second hash value for the second transmission data, encrypts the second transmission data using the second encryption key to generate encrypted second transmission data, and transmits the second hash value and the encrypted second transmission data to the communication device, as recited in independent claims 2.

Devadas further fails to disclose a communication device that decrypts the encrypted second transmission data using the first encryption key, calculates using the first hash key a second hash value for the decrypted second transmission data, and determines that the second

transmission data is not tampered when the received second hash value matches the calculated second hash value, as recited in independent claims 2.

Instead, Devadas merely teaches that a hash module h2 193 generates one secret key based on the old response (paragraph [0212] and Fig.21). In other words, in Devadas, the one secret key is generated NOT based on both the old response and the new response, and two types of keys are not generated based on the one old response. Devadas also merely teaches that encryption and MAC module 195 encrypts the message and generates a MAC for the encrypted message using the one secret key (paragraph [0212] and Fig.21). In other words, in Devadas, the message is encrypted using the one secret key, and the MAC for the encrypted message is calculated using the same one secret key.

Thus, Devadas does not contain any disclosures regarding a device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to another device, as recited in, for example, independent claim 1 .

As Devadas fails to disclose the above features, Devadas does not contain any disclosures regarding a system which includes a device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from another device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value, as recited in, for example, independent claim 1. Additionally, one or more of the above features noted above in independent claims 1 and 2 are similarly recited independent claims 11 and 12.

Moreover, in the Office Action, the Examiner asserts that in the claimed invention there is no requirement for the encryption key and hash key to be different. However, by the present

amendments, the Applicants have amended claims 1-2, and 11-12 to recite "the first encryption key being distinct from the first hash key" and "the second encryption key being distinct from the second hash key" therein.

If the first encryption key and the first hash key are the same key, the first device calculates using the first encryption key a first hash value for the first transmission data and encrypts the first transmission data using the first encryption key. In this case, the first device transmits the first hash value (calculated using the first encryption key) and the encrypted first transmission data (encrypted using the same first encryption key) to the second device. When the transmitted first hash value is analyzed by an unauthorized user, the first encryption key can be leaked out to the unauthorized user.

In this case, the security cannot be protected for the encrypted first transmission data. In other words, when the first encryption key and the first hash key are the same key, the first encryption key can be leaked out to the unauthorized user based on the transmitted first hash value. In the result, the encrypted first transmission data can be decrypted by the unauthorized user, based on the first hash value transmitted with the encrypted first transmission data. On the other hand, the pending claims recite the first encryption key and the first hash key that is distinct from the first encryption key, calculates using the first hash key a first hash value for the first transmission data and encrypts the first transmission data using the first encryption key. Then, the first device transmits the first hash value (calculated using the first hash key) and the encrypted first transmission data (encrypted using the first encryption key) to the second device.

Additionally, when the first hash value is analyzed by the unauthorized user, the unauthorized user cannot obtain the first encryption key, and thus the security can keep to be protected for the encrypted first transmission data. For the same reasons, the second encryption key is required to be distinct from the second hash key, at the second device side. Therefore, the second device can determine that the first transmission data is not tampered when the received first hash value matches the calculated second hash value (calculated using the second hash key), while the security can be protected for the encrypted first transmission data.

Therefore, the present invention (as recited in independent claims 1, 2, 11 and 12) is

clearly distinguished over Diffie and Devadas. Accordingly no combination of Diffie and Devadas would result in, or otherwise render obvious, independent claims 1, 2, 11 and 12. Additionally, no combination of Diffie and Devadas would result in, or otherwise render obvious, claims 5 and 10 at least by virtue of their dependencies from independent claim 2.

B. In the Office Action, Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Diffie in view of Devadas and Morais et al. (US 2003/0093669, hereafter "Morais"). Claim 4 depends from claim 2. As noted above, Diffie and Devadas fail to disclose or suggest all the features recited in independent claim 2. Additionally, after a detailed review of Morais, the reference fails to overcome the deficiencies noted above in Diffie and Devadas.

More specifically, in the Office Action, the Examiner relies on Morais regarding that which the Examiner admits is lacking in the Diffie and Devadas, by asserting that Morais discloses that the hash key can be used to produce shared key and the notion of producing infers that the hash key and the secret key are not the same.

Morais discloses a network architecture for console-based gaming systems that enables secure communication among multiple game consoles over a local area network. The system architecture supports a three-phase secure communication protocol. In a first phase, a client console stores a secret key 402, and a title key 404 is stored as part of a game title. The LAN key generator 406 generates a LAN key 408 using the secret key 402 and the title key 404. The broadcast key generator 410 generates a title broadcast key 412 and a title broadcast signature key 414 using the LAN key 408 (see paragraphs [0043]-[0047] and Fig.4).

In a second phase, the client console encrypts a request using the title broadcast key 412, signs the request using the title broadcast signature key 414, and broadcast the encrypted and signed request to other consoles on the LAN. Consoles running the same game title will recognize the request because they can generate the same set of the title broadcast key 412 and the title broadcast signature key 414. Consoles running different game titles will disregard the request. If the one host console is running the same game title, the host console authenticates the request using the same title broadcast signature key 414, and decrypts the request using the same

title broadcast key 412. The host console decides whether to allow the requesting client console to participate in the network game. Factors affecting the game include the number of current players, number players supported by the game, and current status of the game (i.e., just beginning, middle of session, etc) (see paragraphs [0048]-[0055] and Fig.5).

However, Morais fails to disclose a device that generates the first encryption key and a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to another device. In particular, Morais fails to disclose a device that transmits the first hash value and the encrypted first transmission data to another device.

Rather, Morais merely teaches that each console running the same game title generates the same set of the title broadcast key 412 and the title broadcast signature key 414 (see paragraph [0053]). Thus, in Morais, the console broadcasts only the encrypted and signed request to other consoles on the LAN, without calculating using the title broadcast key 412 or the title broadcast signature key 414 a hash value for the encrypted and signed request and without transmitting the calculated hash value.

Morais also fails to disclose a device that generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matches the calculated second hash value.

In particular, Morais fails to disclose a device that determines that the first transmission data is not tampered when the received first hash value (that is received with the encrypted first transmission data) matches the calculated second hash value (that is calculated using the second hash key). Rather, the host console merely authenticates the request using only the

title broadcast signature key 414 that the host console itself generates (see paragraphs [0053]-[0054]). In Morais, the console does not broadcast, to other consoles on the LAN, a hash value calculated using the title broadcast key 412 or the title broadcast signature key 414 when the console broadcasts the encrypted and signed request.

Therefore, the Applicants submit that even if one of ordinary skill in the art combined the teaching of Diffie, Devadas and Morais (as suggested by the Examiner), the combination still fails to arrive at the present invention, as recited in independent claims 2 and from which claim 4 depends. Accordingly, no combination of Diffie, Devadas and Morais would result in, or otherwise render obvious, claim 4 at least by virtue of its dependency from independent claim 2.

II. Conclusion

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue. The Examiner is invited to contact the undersigned attorney by telephone to resolve any remaining issues.

Respectfully submitted,

Yuichi FUTA et al.

/Mark D. Pratt/

By: 2009.02.18 16:08:55 -05'00'

Mark D. Pratt
Registration No. 45,794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
February 18, 2009